

What is claimed is:

- 1 1. A method for validating a restored message, comprising:
2 generating an entry in a signature log for a message, wherein said entry
3 comprises cryptographic information associated with said message;
4 when said message is lost, generating said restored message responsive to
5 a request; and
6 validating said restored message using said signature log.
- 1 2. The method of claim 1 wherein said signature log comprises a
2 hysteresis signature.
- 1 3. The method of claim 1 wherein said cryptographic information
2 comprises a digital signature.
- 1 4. The method of claim 3 wherein said digital signature is generated
2 using information from a previous signature log entry.
- 1 5. A system for recovering and validating user information,
2 comprising:
3 a user system comprising a signature log, said signature log comprising
4 cryptographic information associated with said user information;
5 a recovery system coupled with said user system via a communications
6 network for restoring user information; and
7 a validity system coupled with said user system via said communications
8 network for validating restored user information using said signature log.
- 1 6. The system of claim 5 wherein said user information comprises a
2 log entry of said signature log.
- 1 7. The system of claim 5 wherein said user information comprises a
2 user message.
- 1 8. The system of claim 5 wherein said cryptographic information
2 comprises a hash value.

09816777-032201

1 9. The system of claim 5 wherein said signature log comprises a first
2 log entry of said signature log determined in part by a second log entry of said signature
3 log.

1 10. A system for determining if a user message is valid, said system
2 comprising:
3 a user computer system having a log, said log comprising a log entry
4 related to a message sent by said user, wherein said log entry has a digital signature
5 comprising information related to a previous log entry of said log; and
6 a validation unit coupled to said user computer system for validating said
7 user message using said log.

1 11. The system of claim 10 further comprising a collection unit
2 responsive to said validation unit for retrieving said user message, when said user
3 message is lost.

1 12. The system of claim 10 further comprising a collection unit
2 responsive to said validation unit for retrieving a copy of said message from a receiver of
3 said message, when said user message is lost.

1 13. The system of claim 10 further comprising a publication unit for
2 publishing a selected log entry of said log.

1 14. The system of claim 13 wherein said selected log entry is used in
2 validating said user message.

1 15. The system of claim 13 wherein publication unit is selected from a
2 group consisting of a newspaper publisher or a Web site.

1 16. The system of claim 10 further comprising a notary unit for
2 registering a selected log entry of said log.

1 17. The system of claim 10 further comprising a log chain crossing
2 unit coupled to said user computer system and a second user computer system for
3 recording transactions between said user computer system and said second user computer
4 system.

09816777, 032201
T022220 2229T86

1 18. The system of claim 10 further comprising a log chain crossing
2 unit coupled to said user computer system and a second user computer system for
3 facilitating transactions between said user computer system and said second user
4 computer system.

1 19. A computer readable data transmission medium containing a data
2 structure for validating message information comprising:

- 3 a first portion having a hash of a user message;
- 4 a second portion having a hash of a signature log entry; and
- 5 a digital signature based on said first portion and said second portion.

1 20. The computer readable data transmission medium of claim 19
2 wherein said signature log entry is related to another user message prior to said user
3 message.

1 21. The computer readable data transmission medium of claim 19
2 further comprising a third portion having a timestamp.

1 22. A method, using a computer, for generating a signature log
2 comprising a plurality of log entries, said method comprising:
3 generating a first log entry of said plurality of log entries, said first log
4 entry comprising a first cryptographic value associated with a first user message; and
5 generating a second log entry of said plurality of log entries, said second
6 log entry comprising a second cryptographic value associated with said first log entry, a
7 third cryptographic value associated with a second user message, and a digital signature.

1 23. The method of claim 22 wherein said digital signature is formed
2 using information including said second cryptographic value and said third cryptographic
3 value.

1 24. The method of claim 22 wherein said second cryptographic value is
2 a hash of said first log entry.

1 25. The method of claim 22 wherein said second log entry further
2 comprises a timestamp.

0981677-03201

1 26. A data structure stored in a computer readable medium for
2 validating a selected user message of a plurality of user messages, comprising:
3 a first hash of a first log entry, wherein said first log entry comprises a
4 second hash of a first user message of said plurality of user messages;
5 a third hash of said selected user message of said plurality of user
6 messages; and
7 a digital signature of said first hash combined with said third hash.

1 27. In a computer system, a method for validating a selected log entry
2 by using a signature log having a plurality of recorded log entries, said method
3 comprising:
4 computing a cryptographic value for said selected log entry ; and
5 determining if said cryptographic value is part of a first recorded log entry
6 of said plurality of recorded log entries.

1 28. The method of claim 27 wherein said selected log entry
2 corresponds to a second recorded log entry of said plurality of recorded log entries
3 sequentially prior to said first recorded log entry.

1 29. A system for preventing repudiation of a transaction by one of a
2 plurality of user computer systems, said system comprising:
3 a first user of said plurality of user computer systems;
4 a second user of said plurality of user computer systems performing said
5 transaction with said first user; and
6 a log chain crossing computer responsive to a request by either said first or
7 said second user to record said transaction, said record comprising a hysteresis
8 signature of said transaction.

1 30. A method using a computer system for registering a log entry of a
2 user by an officially recognized entity, comprising:
3 maintaining a signature log chain by said officially recognized entity,
4 wherein a first log entry of said signature log chain is related to a previous second log
5 entry of said signature log chain;
6 receiving from said user a user log entry;

00816777.03201

7 generating a cryptographic value associated with said user log entry; and
8 generating a third log entry of said signature log chain, wherein said third
9 log entry comprises said cryptographic value.

1 31. The method of claim 30 wherein a selected log entry of said
2 signature log chain is published.

1 32. The method of claim 30 wherein said officially recognized entity is
2 a notary.

1 33. A method for validating a user data item by a computer system
2 using a user's signature log, comprising:
3 receiving said user's signature log;
4 validating a cryptographic value associated with said user data item is in a
5 first log entry in said user's signature log;
6 determining a second log entry in said user's signature log that is
7 checkpointed;
8 verifying said first log entry by back chaining from said second log entry
9 to said first log entry; and
10 returning a result to said user.

1 34. A method, using a computer system, for recovering a data item
2 between two points in time, comprising:
3 receiving a request from a user to recover data between two points in time,
4 wherein said data item is between said two points in time;
5 receiving from a data recovery unit said data item and associated signature
6 log entry;
7 validating said data item using said associated signature log entry; and
8 if said data item is validated, sending said data item to said user.

1 35. A system for validating a user message, comprising:
2 an input module for receiving a signature log from a user, said signature
3 log comprising a plurality of related log entries;
4 a cryptographic module for generating a cryptographic value from said
5 user message; and

09816777-032201

6 a verifying module for validating said cryptographic value is in said
7 signature log.

1 36. The system of claim 35 further comprising a log verifying module
2 for determining if a first log entry of said plurality of related log entries is compromised,
3 said determining comprising:

4 selecting a second log entry of said plurality of related log entries
5 subsequent to said first log entry;

6 hashing said first log entry to give a hash value; and

7 validating said hash value is part of said second log entry.

1 37. A computer program product for validating a restored message,
2 comprising:

3 code for generating an entry in a signature log for a message, wherein said
4 entry comprises cryptographic information associated with said message;

5 when said message is lost, code for generating said restored message
6 responsive to a request;

7 code for validating said restored message using said signature log; and
8 a computer usable medium for embodying said codes.

1 38. The computer program product of claim 37, wherein said computer
2 usable medium is a storage medium.

1 39. The computer program product of claim 37, wherein said computer
2 usable medium is a carrier wave.

1 40. A computer data signal embodied in a carrier wave for validating a
2 restored message, comprising:

3 program code for generating an entry in a signature log for a message,
4 wherein said entry comprises cryptographic information associated with said message;

5 when said message is lost, program code for generating said restored
6 message responsive to a request; and

7 program code for validating said restored message using said signature
8 log.

0901677 03201
T0228 79T860